Review: Biometrics Technologies Measure Up (Part 2/3)

November 19 2005

(Part 2/3) (Part 1) Biometrics technologies have come a long way from a slow start in the early 80s. Now they can be found almost anywhere and soon, almost everywhere.

Eye Scanners

Iris scanning technology was first thought of in 1936 by ophthalmologist Frank Burch. He noticed that each person's iris – the part of the eye that gives color – is unique. It wasn't till 1994 when the algorithm for detecting these differences was patented by John Daugman of Iridian

Technologies.

Iris scans analyze the features in the colored tissue surrounding the pupil. There are many unique points for comparison including rings, furrows and filaments. The scans use a regular video camera to capture the iris pattern.

The user looks into the device so that he can see the reflection of his own eye. The device captures the iris pattern and compares it to one in a database. Distance varies, but some models can make positive identification at up to 2 feet. Verification times vary - generally less than 5 seconds - but only require a quick glance to activate the identification process.

To prevent a fake eye from being used to fool the system, some models vary the light levels shone into the eye and watch for pupil dilation – a fixed pupil means a fake eye.

Iris scanners are now in use in various military and criminal justice facilities but have never gained the wide favor that fingerprint scanners

now enjoy even though the technology is considered more secure. Devices tend to be bulky in comparison to fingerprint scanners.

Retinal scanners are similar in operation but require the user to be very close to a special camera. This camera takes an image of the patterns created by tiny blood vessels illuminated by a low intensity laser in the back of the eye – the retina.

Retinal scans are considered impossible to fake and these scanners can be found in areas needing very high security. High cost and the need to actually put your eye very close to the camera prevent them from being used more widely.

Face Recognition

Never forget a face? Why? Because each persons face is unique – enough so that this new technology promises to change they way people are identified. It also has some serious ethical and privacy concerns.

Unlike the other technologies mentioned that require the user to participate actively, this technology can do everything without you ever

being aware of its presence.

It works by taking a picture of your face and comparing things like the distance between your eyes, the width of your mouth and up to 50 other defining facial traits. It then searches a database for matches, displaying those that are similar or exactly equal to an operator.

During the 2000 Olympics in Sidney, Australia, police identified two drug traffickers from Mexico wanted in the US. They followed them to the airport then alerted US authorities who picked them up when their return flight made a refueling stop in Hawaii. They had been traveling with high quality faked papers, so were quite surprised when the FBI led them off in cuffs.

The suspects had unwittingly stumbled into the police's hands during a visit to the main sports arena. Australian authorities had just installed a face identification system in order to thwart possible terrorist attacks. They loaded the system with all known terrorist's and criminal's photos from a huge database. When the drug traffickers passed through the gates – they, along with hundreds of thousands of others, were imaged and identified.

This same technology is used by London police to identify known criminals in commercial areas like malls. Large retail chains have also been using this technology to spot shoplifters although some have removed it after privacy advocates and customers objected.

Recent studies have shown that even in optimal conditions these systems, which are still being developed, have failure rates of close to 40% making them unsuitable for primary identification without some other form of verification.

However, their ability to work with existing digital and CCTV

surveillance systems makes them attractive retrofits. Just install a computer with the face recognition software and photo database, connect it to your cameras and your ready to identify possible malefactors.

More reliable systems are available using stereoscopic cameras. Two or more cameras work together to construct a 3D image in a computer. This allows for more facial features to be cataloged thus greatly reducing error rates. It does, however, require active participation from the users to get original pictures for the database – for the time being. Future models will no doubt be able to take pictures from behind two way glass.

Errors caused by camera angle and poor image quality, however, require more investment and care in camera placement. Most systems can deal with things like hats, sunglass and acute image angles, but they increase the possibility of false identification.

Privacy advocates cite 4th Amendment protection against unreasonable search and seizures. Law enforcement agencies say it's just an extension of their own observational powers and an unobtrusive way to identify people.

To Be Continued ... (in part 3: Pattern Recognition) (Part 1)